THE INDUSTRIAL IMMUNE SYSTEM

Using Machine Learning for Next Generation ICS Security

Jeff Cornelius, Ph.D., EVP, Darktrace

DARKTRACE

Darktrace Background

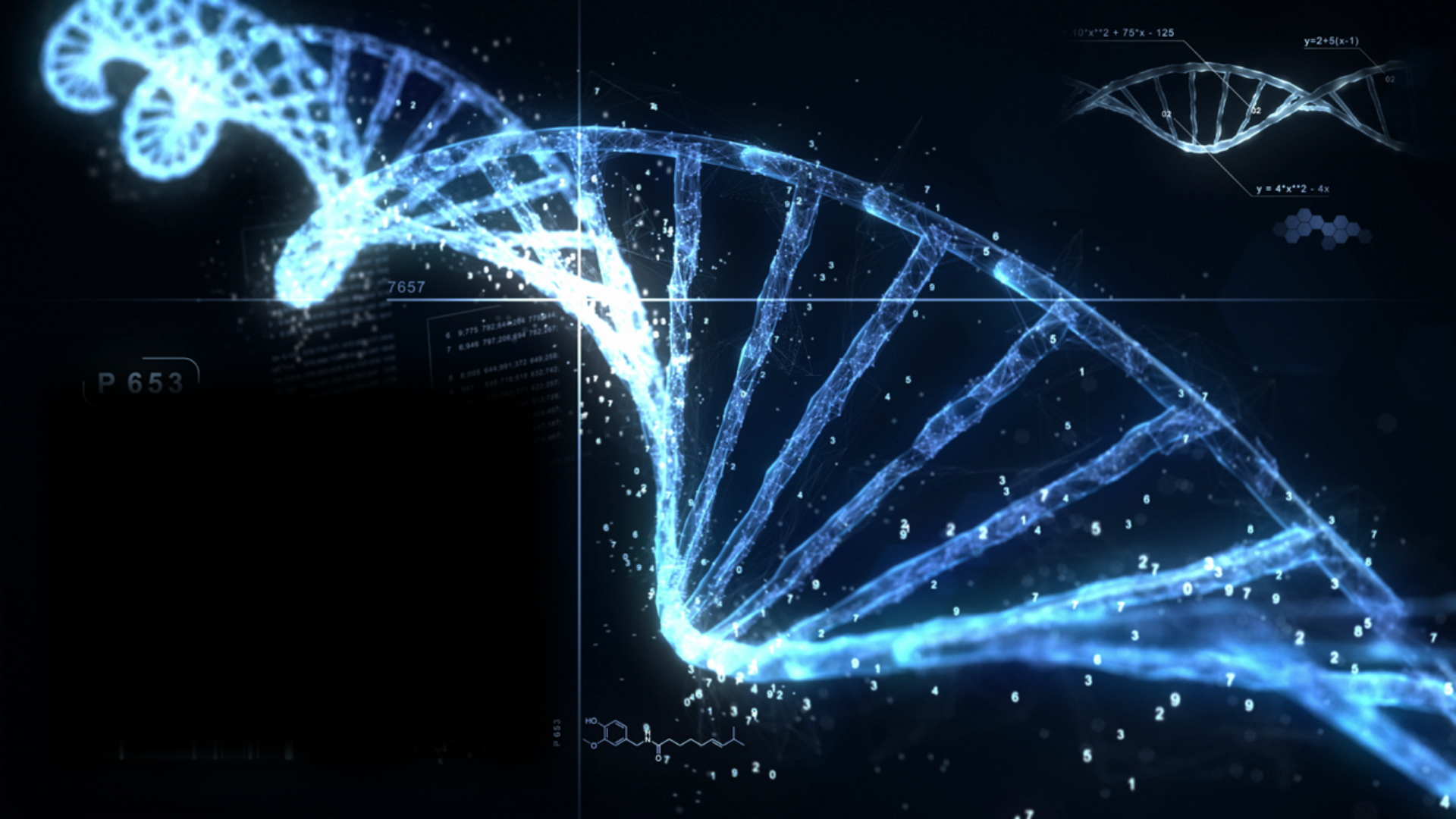
- Founded by world-leading mathematicians, from the University of Cambridge, and cyber operations experts
- Powered by machine learning and mathematics
- 600% year-on-year growth
- HQs in San Francisco, and Cambridge, UK

The Challenges of OT Security

- The evolution of networking in the industrial / production world has been ad-hoc
- Cyber security has not been factored in – retrofitting is difficult
  - Vendor-specific security efforts prove challenging
- Process control software is often running on unpatched (even non-supported) operating systems
- Migration to a common networking architecture opens up opportunities for cost saving but introduces risk (especially if multi-site, multi-national, multi-vendor)

The Modern Threat Landscape

- Sharp increase in attacks in ICS environments
- Conversion of IT and OT networks
- Perimeter defenses and airgapping not enough
- Traditional solutions don’t work in ICS/SCADA environments


10*x**2 + 75*x - 125
y=2+5(x-1)
y = 4*x**2 - 4x
7657
P 653

The Industrial Immune System: Proven to Work

Learns ‘self’ in real time

For every individual user, device and network, using unsupervised machine learning

Finds the threats that get through

Detects both insider and sophisticated external threats, from within the network

100% visibility

Visualizes entire network, including traditional and non-traditional IT, allows for investigations

Scalable

Largest deployment has over 1 million users

All networks & devices

Works on physical and virtual networks, cloud, ICS/OT

Machine Learning is Hard to Get Right

- No two networks are alike – needs to work in every network
- Needs to work without customer configuration or tuning of models
- Needs to support teams with varying security & math skills
- Must deliver value immediately, but keep learning and adapting as it goes
- Must have linear scalability
- Cannot rely on training sets of data

Conclusion

- The intrusion of your networks is inevitable
- Legacy approaches do not work – based on rules & signatures
- Advanced understanding of digital infrastructure based on unsupervised machine learning and mathematics
- Focus team’s effort only on true anomalies and suspicious activity
- Early detection of threats in ICS environment critical to resiliency.

Threat Examples

DARKTRACE

Threat Example: Power Station Subcontractor

- Energy firm with confidential information
- Subcontractor transferred information to a home router
- Information related to cabling and backups at one of the company's power stations, and projects for tender
- Detected as anomalous – abnormal data transfers

Threat Example: Compromised Internal Server

- Suspicious remote-control connection discovered
- External computer was in control an internal server
- Compromised internal server was transmitting messages to a computer in Asia

Threat Example: Unauthorized Use of Internal Device

- Internal server behaved in a way that seemed like it was being controlled remotely
- This behavior was unknown to security team
- No obvious reason for anomalous activity
- Emerging security risk

Threat Example: Internal Reconnaissance '

- Suspicious scanning activity at an Estonian network operator company
- A device outside the ICS trying to connect
- Abnormal behavior not connected to routine network maintenance
- Serious security risk

Case Study: Drax '

- Drax is part of critical national infrastructure
- Provides 8% of Europe's energy
- Needed to protect corporate IT & ICS environments
- Key partner in developing Darktrace's SCADA capability
- Uses Enterprise & Industrial Immune Systems to monitor both IT & OT
- Continuous monitoring of networks & anomalies
- Ability to investigate and mitigate threats in real time

"Darktrace's technology has identified threats with the potential to disrupt our systems"

Martin Sloan, Head of Safety & Security at Drax Group

Thank you

jeff.cornelius@darktrace.com
682-888-2111 m

DARKTRACE